ROBSON HOUSE

Online safety Policy

Policy Owner	Robson House
Approving Body	Robson House Management Committee
Date Approved	September 2021
Effective Date	September 2021
Review Date	September 2022
Version	7

Contents

Key Contacts

Online safety: the issues

Robson House online safety strategies

Online safety policies

Remote Learning

Responding to incidents

Sanctions for misuse of ICT

Appendices:

Appendix 1: Acceptable use policy for children
Appendix 2: Acceptable use policies for staff
Appendix 3: Online safety incident report form

Key Contacts

Name of school: Robson House

Executive Headteacher:
Bavaani Nanthabalan
ehead@netley.camden.sch.uk

Online safety co-ordinator:
Alyson Dermody Palmer
alyson.dermody.palmer@camden-plss.camden.sch.uk

Nominated LGFL contact:
Darryl Jones
darryl.jones@camden-plss.camden.sch.uk

IT systems/ data manager:
Darryl Jones
darryl.jones@camden-plss.camden.sch.uk

Nominated Management Committee member:
Jane Walby

London Borough of Camden

Child protection lead officer and Local Authority Designated Officer (LADO)
Sophie Kershaw/John Lawrence-Jones
020 7974 4556

Children's Contact Service/ MASH team:
LBCMASHadmin@camden.gov.uk
Manager:Jade Green
020 7974 1553/3317
Fax: 020 7974 3310

Camden online safety officer:
Jenni Spencer
020 7974 2866

Prevent Education Officer:
Name: Jane Murphy
Tel: 020 7974 1008

Information on internet technology

Introduction

It is commonly acknowledged that the educational and social benefits for children in using the internet should be promoted, but that this should be balanced against the need to safeguard children against the inherent risks from internet technology. Further, schools need to be able to teach children to keep themselves safe whilst on-line.

This document provides guidance to enable these aims to be achieved and support staff to recognise the risks and take action to help children use the internet safely and responsibly.

The online safety policy is available on the school's website.

Benefits and risks

Computing covers a wide range of activities, including access to information, electronic communications and social networking.

As use of technology is now universal, it is imperative that children learn computing skills in order to prepare themselves for the working environment and that the inherent risks are not used to reduce children's use of technology. Further, the educational advantages of computing need to be harnessed to enhance children's learning.

The risk associated with use of technology by children can be grouped into 4 categories.

Content

The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism, suicide or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.

Contact

Chat rooms, gaming sites and other social networking sites can pose a real risk to children as users can take on an alias rather than their real names and can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them.

Children may not be aware of the danger of publishing or disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent.

The internet may also be used as a way of bullying a child, known as online bullying. More details on this can be found in section 4 of this policy.

Commerce

Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences, such as fraud or identity theft, for themselves and their parents. They may give out financial information, for example, their parent's credit card details, in response to offers for goods or services without seeing the fraudulent intent. Contact via social networking sites can also be used to persuade children to reveal computer passwords or other information about the family for the purposes of fraud.

Culture

Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:

- becoming involved in inappropriate, anti-social or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people

- using information from the internet in a way that breaches copyright laws

- uploading personal information about themselves, including photographs, on social networking sites without realising they are publishing to a potentially global audience

- online bullying (see section 4 for further details)

- use of mobile devices to take and distribute inappropriate images of the young person (sexting) that cannot be removed from the internet and can be forwarded on to a much wider audience than the child intended.

Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their health, social and emotional development and their educational attainment. They may visit sites that advocate extreme and dangerous behaviour such as self-harm or suicide or violent extremism, and more vulnerable children may be at a high degree of risk from such sites. All children may become desensitised to pornography, violence, sex and drug use or self-harm by regularly viewing these on-line.

Robson House online safety strategies

Whole school approach

Computing is a key part of the school curriculum as well as a key element of modern communications technology that is widely used, and one of the key aims of computing is to ensure that children are aware of online safety messages. This is part of the school's responsibility to safeguard and promote the welfare of children, as well as the duty of care to children and their parents to provide a safe learning environment.

At Robson House we consider the following in order to ensure a holistic approach to online safety:

- Staff are made aware that online safety is an element of many safeguarding issues as technology can be used to aid many forms of abuse and exploitation, for example sexual harassment and cyberbullying, and aware of the use of technology in peer on peer abuse.

- When developing new policies, we ensure online safety and the impact of technology is considered and what safeguards need to be put in place, for example when developing policies around behaviour and staff conduct.

- Ensure that consistent messages are given to staff and pupils and that everyone understands the online safety policy: staff receive suitable training around online safety and similar messages are taught to children.

- Staff are aware of the importance of ensuring their own use of technology complies with school policies, particularly in terms of contact with children, and we ensure there are clear policies available to staff on expectations for online behaviour.

- There is a clear link between the online safety policy and the behaviour policy that sets out expected standards for children's online behaviour and expected sanctions for breaches.

- Our online safety policy is reviewed regularly and staff training refreshed in order to ensure that they remain relevant in the face of changing technologies.

Schools should refer to:

DfE non-statutory guidance on teaching online safety:
https://www.gov.uk/government/publications/teaching-online-safety-in-schools

DfE statutory guidance on RSE: https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

Purpose and description

Robson House has an online safety strategy in place based on a framework of policy, practice, education and technological support that ensures a safe online learning environment that maximises the educational benefits of ICT whilst minimising the associated risks. Its purpose is to:

- promote the use of technology within the curriculum
- protect children from harm
- safeguard staff in their contact with children and their own use of the internet
- ensure the school fulfils its duty of care to children
- provide clear expectations for staff and children on acceptable use of the internet.

In particular, Robson House ensures the following:

- A safe internet platform (London Grid for Learning Platform) that provides filtering software to block access to unsuitable sites, anti-virus software and monitoring systems.
- A culture of safe practice underpinned by a strong framework of online safety policy that ensures everyone is aware of expected standards of on-line behaviour.
- Children are taught to keep themselves and others safe on-line and use technology responsibly; this should be achieved by working in partnership with parents and carers and raising awareness of the potential risks of internet use.

Roles and responsibilities

A successful online safety strategy needs to be inclusive of the whole school community, including all staff and members of the Management Committee and others, and forge links with parents and carers. The strategy must have the backing of the Management Committee, should be overseen by the executive head teacher and be fully implemented by all staff.

Executive head teacher’s role

The executive head teacher has ultimate responsibility for online safety issues within Robson House including:

- the overall development and implementation of the school’s online safety policy and ensuring the security and management of online data
- ensuring that online safety issues are given a high profile within the school community

- linking with the members of management committee and parents and carers to promote online safety and forward the school's online safety strategy
- ensuring online safety is embedded in staff induction and training programmes
- deciding on sanctions against staff and children who are in breach of acceptable use policies and responding to serious incidents involving online safety

The members of management committee members' role

The members of the Management Committee have a statutory responsibility for child safety and is therefore aware of online safety issues, providing support to the executive head teacher and heads of school in the development of the school's online safety strategy. The Management Committee should ensure that there are policies and procedures in place to keep children safe online and that these are reviewed regularly.

The members of the Management Committee members are subject to the same online safety rules as staff members and should sign an Acceptable Use Agreement in order to keep them safe from allegations and ensure a high standard of professional conduct. In particular, Management Committee members always use business email addresses where possible when conducting school business.

Online safety co-ordinator's role

Robson House has a designated online safety co-ordinator (Alyson Dermody Palmer) who is responsible for co-ordinating online safety policies on behalf of the school. The co-ordinator is one of the heads of school, as well as one of the designated safeguarding leads. Given the issues associated with online safety, it is appropriate for the designated safeguarding lead to be the school's online safety co-ordinator.

The online safety co-ordinator has the knowledge, experience and authority to carry out the following:

- develop, implement, monitor and review the school's online safety policy
- to ensure that staff and children are aware that any online safety incident should be reported to her
- ensure online safety is embedded in the curriculum
- provide the first point of contact and advice for school staff, members of management committee, children and parents
- liaise with the school's network manager, the executive head teacher and nominated governor to ensure the school remains up to date with online safety issues and to address any new trends, incidents and arising problems
- assess the impact and risk of emerging technology and the school's response to this in association with IT staff and learning platform providers
- raise the profile of online safety awareness with the school by ensuring access to training and relevant online safety literature
- ensure that all staff and children have read and signed the acceptable use policy (AUP)
- report annually to the management committee on the implementation of the school's online safety strategy
- maintain a log of internet related incidents and co-ordinate any investigation into breaches

- report all incidents and issues to Camden’s online safety officer.

In line with the Ofsted recommendation that the online safety co-ordinator receives recognised training CEOP or E-PICT in order to carry out their role more effectively. Alyson Dermody Palmer and Carla Stooke have attended CEOP training .All staff completed the CEOP remote training in January 2021.

Camden representative’s role

Their role is:

- the maintenance and monitoring of the school internet system including anti-virus and filtering systems
- carrying out monitoring and audits of networks and reporting breaches to the online safety co-ordinator
- supporting any subsequent investigation into breaches and preserving any evidence.

Role of school staff

All school staff have a dual role concerning their own internet use and providing guidance, support and supervision for children. Their role is:

- adhering to Robson House’s online safety and acceptable use policy and procedures
- communicating Robson House’s online safety and acceptable use policy to children
- keeping children safe and ensuring they receive appropriate supervision and support whilst using the internet
- planning use of the internet for lessons and researching on-line materials and resources
- reporting breaches of internet use to the online safety co-ordinator
- recognising when children are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the online safety co-ordinator
- teaching the online safety and digital literacy elements of the new curriculum.

Designated safeguarding leads

Where any online safety incident has serious implications for the child’s safety or well-being, the matter is referred to one of the designated people for safeguarding who decides whether or not a referral should be made to Children’s Safeguarding and Social Work or the Police.

Children with Special Educational Needs and Disabilities (SEND)

Children with learning difficulties or disability may be more vulnerable to risk from use of the internet and may need additional guidance on online safety practice as well as closer supervision. As all the children at Robson House have special educational needs, school staff are responsible for assessing children needs individually and providing extra support for these children:

- link with the online safety co-ordinator to discuss and agree whether the safeguarding systems on the internet are adequate for the children
- where necessary, liaise with the online safety co-ordinator and the IT service to discuss any requirements for further safeguards to the school IT system or tailored resources and materials in order to meet the needs of the children
- ensure that the school's online safety policy is adapted to suit the needs of the children
- liaise with parents, carers and other relevant agencies in developing online safety practices for the children
- keep up to date with any developments regarding emerging technologies and online safety and how these may impact on the children

Working with parents and carers

At Robson House we involve parents and carers in the development and implementation of online safety strategies and policies; This is important as most children will have internet access at home or own mobile devices and might not be as closely supervised in its use as they would be at school.

Therefore, parents and carers need to know about the risks so that they are able to continue online safety education at home and regulate and supervise children's use as appropriate to their age and understanding.

The executive head teacher, heads of school, members of the management committee and the online safety co-ordinator have considered what strategies to adopt in order to ensure parents are aware of online safety issues and support them in reinforcing online safety messages at home. Regular online safety workshops for parents, letters about specific issues, as well as individual work with parents are some of the strategies used at Robson House. The CSCB online safety leaflet for parents is available on the school website. https://cscp.org.uk/parents-and-carers/online-safety/

Parents are provided with information on computing and the Robson House's online safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within the school as well as the school's expectations regarding their behaviour. Parents are also encouraged to contact the school's online safety co-ordinator or child and family mentors if they have any concerns about their child's use of technology.

Online safety policies

Accessing and monitoring the system

- Access to Robson House's internet system is via individual log-ins and passwords for staff and children wherever possible. Visitors can have permission from the heads of school or online safety co-ordinator to access the system and be given a separate visitors log-in.

- The online safety co-ordinator keeps a record of all log-ins used within the school for the purposes of monitoring and auditing internet activity.
- Staff are required to change their password every six months
- Network and technical staff responsible for monitoring systems are supervised by a senior member of their management team.
- The online safety co-ordinator and school staff carefully consider the location of internet enabled devices in classrooms and teaching areas in order to allow an appropriate level of supervision of children depending on their age and experience.

Confidentiality and data protection

- Robson House will ensure that all data on its IT system is held in accordance with the principles of the Data Protection Act 1998. Data will be held securely and password protected with access given only to staff members on a “need to know” basis
- Children’s data that is sent to other organisations will be encrypted and sent via a safe and secure system. Any breaches of data security should be reported to the executive head immediately

Acceptable use policies

- All internet users within Robson House are expected to sign an acceptable use agreement that sets out their rights and responsibilities and incorporates Robson House’s online safety rules regarding their internet use.

- At Robson House, acceptable use agreements are signed by parents on their child’s behalf at the same time that they give consent for their child to have access to the internet in school (see appendix 1).

- Staff are expected to sign an acceptable use policy on appointment and this will be integrated into their general terms of employment (see appendix 2).

- The online safety co-ordinator will keep a copy of all signed acceptable use agreements.

Teaching online safety

Responsibility

One of the key features of Robson House’s online safety strategy is teaching children to protect themselves and behave responsibly while on-line. There is an expectation that over time, children will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.

- Overall responsibility for the design and co-ordination of online safety education lies with the executive head teacher, heads of school and the online safety co-ordinator, but all staff play a role in delivering online safety messages.

- The online safety co-ordinator is responsible for ensuring that all staff have the knowledge and resources to enable them to do so.

- Teachers are primarily responsible for delivering an ongoing online safety education in the classroom as part of the curriculum.

- Rules regarding safe internet use are posted up in all classrooms and teaching areas where computers are used to deliver lessons.

- The start of every lesson where computers are being used is used as an opportunity to remind children of expectations on internet use and the need to follow basic principles in order to keep safe.

- Teachers use PSHE lessons as a forum for discussion on online safety issues to ensure that children understand the risks and why it is important to regulate their behaviour whilst on-line.

- School staff are aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.

- School staff ensure that the school's policy on children's use of their own mobile phones and other mobile devices in school is adhered to.

Content

Children are taught all elements of online safety included in the computing curriculum so that they:

- use technology safely and respectfully, are keeping personal information private; can identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems
- are responsible, competent, confident and creative users of information and communication technology.

The children are taught all elements of online safety included in Statutory Relationships Education:

- about different types of bullying (including cyberbullying), the impact of bullying, responsibilities of bystanders (primarily reporting bullying to an adult) and how to get help

- that people sometimes behave differently online, including by pretending to be someone they are not.
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- how information and data is shared and used online.

The children are taught all elements of online safety included in Statutory Health Education:

- that bullying (including cyberbullying) has a negative and often lasting impact on mental wellbeing
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health
- how to be a discerning consumer of information online including understanding that information, including that from search engines is ranked, selected and targeted
- where and how to report concerns and get support with issues online.

Staff training and conduct

- All staff and management committee members receive training with regard to IT systems and online safety as part of their induction and this includes a meeting with the online safety co-ordinator and the network manager

- Staff also attend specific training about online safety from either CSCB or Camden City Learning Centre (CCLC) so that they are aware of the risks and actions to take to keep children safe online. School management ensure that staff receive regular update training so that they can keep up with new developments in technology and any emerging safety issues

- CCLC also provide training to parents/ carers at Robson House

IT and safe teaching practice

School staff are aware of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with children. Staff should refer to the social media policy for school staff for further guidance.

The following points are followed by staff to ensure that their behaviour is not open to misinterpretation and to safeguard them from misplaced or malicious allegations.

- Photographic and video images of children are only taken by staff in connection with educational purposes, for example school trips.

- Staff always use school equipment and only store images on the school computer system,

- Staff take care regarding the content of and access to their own social networking sites and ensure that children and parents cannot gain access to these.

- Staff should ensure that any materials published on their own social networking sites are neither inappropriate nor illegal.

- Staff are particularly careful regarding any comments to do with the school or specific children that are communicated over the internet; remarks that are private may go to a wider audience and raise questions regarding confidentiality.

- Staff do not post any comments about specific children or staff members on their social networking sites or any comments that would bring the school or their profession into disrepute

- Staff will not engage in any conversation with children via instant messaging or social networking sites as these may be misinterpreted or taken out of context.

- Where staff need to communicate with children regarding school work, this should be via the parents or carers or through the Google Classroom and messages should be carefully written to ensure that they are clear, unambiguous and not open to any negative interpretation.

- When making contact with parents or children by telephone, staff should only use school equipment. Child or parent numbers are not stored on a staff member’s personal mobile phone and staff avoid lending their mobile phones to children.

- When making contact with parents or children by email, staff always use their school email address or account. Personal email addresses and accounts such as MSN should never be used.

- Staff ensure that personal data relating to children is stored securely and encrypted if taken off the school premises.

- Where staff are using mobile equipment such as laptops or i-pads provided by the school, they ensure that the equipment is kept safe and secure at all times.

Exit strategy

When staff leave, their line manager liaises with the network manager to ensure that any school equipment is handed over and that PIN numbers, passwords and other access codes to be reset so that the staff member can be removed from the school's IT system.

Safe use of technology

Internet and search engines

- When using the internet, children at Robson House are supervised at all times. Staff at Robson House are aware that often, the most computer-literate children are the ones who are most at risk.

- Children are not allowed to aimlessly "surf" the internet and all use always has a clearly defined educational purpose.

- Despite filtering systems, it is still possible for children to inadvertently access unsuitable websites; to reduce risk, staff at Robson House plan use of internet resources ahead of lessons by checking sites and storing information off-line where possible.

- Where staff at Robson House require access to blocked websites for educational purposes, this is discussed and agreed with the online safety co-ordinator, who liaises with the IT service provider for temporary access. Teachers notify the online safety co-ordinator once access is no longer needed to ensure the site is blocked.

Evaluating and using internet content

Teachers at Robson House teach children good research skills that help them to maximise the resources available on the internet so that they can use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content.

Safe use of applications

School email systems are hosted by an email system that allows content to be filtered and allow children to send emails to others within the school or to approved email addresses externally.

Social networking sites such as Facebook, MySpace and Twitter allow users to publish information about them to be seen by anyone who has access to the site. Generally, these have limited use in schools but children are likely to use these sites at home.

Newsgroups and forums are sites that enable users to discuss issues and share ideas on-line. Some schools may feel that these have an educational value.

Chat rooms are internet sites where users can join in “conversations” on-line;
instant messaging allows instant communications between two people on-line. In most cases, children will use these at home although school internet systems do host these applications.

Gaming-based sites allow children to “chat” to other gamers during the course of gaming. Many of the gaming sites are not properly moderated and may be targeted by adults who pose a risk to children. Consequently, such sites are not accessible via school internet systems

Safety rules

- Access to and use of personal email accounts, unregulated public social networking sites, newsgroups or forums, chat rooms or gaming sites on the school internet system is forbidden and may be blocked. This is to protect children from receiving unsolicited mail or contacts and to preserve the safety of the system from hacking and viruses.

- A clear educational use for emails or social networking sites and forums for on-line publishing is identified, only approved sites are used such as those provided by the IT service provider. Any use of these sites are strictly supervised by the responsible teacher.

- Emails are only be sent via the school internet system to addresses within the school system or approved external address. All email messages sent by children in connection with school business are checked and cleared by the responsible teacher.

- Where teachers wish to add an external email address, this must be for a clear educational purpose and will be discussed with the online safety co-ordinator who will liaise with the learning platform provider.

- Apart from the executive head teacher, and the admin officer individual email addresses for staff or children are not published on the school website.

- Children are taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

- Children are taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence or on social networking sites.

- All electronic communications should be polite; if a child receives an offensive or distressing email or comment, they are instructed not to reply and to notify the responsible teacher immediately.

- Children are warned that any bullying or harassment via email, chat rooms or social networking sites will not be tolerated and will be dealt with in accordance with the Robson House's anti-bullying policy. This includes any correspondence or contact taking place outside the school and/or using non-school systems or equipment.

- Users are made aware that as use of the school internet system is for the purposes of education or school business only, and its use may be monitored.

- In order to teach children to stay safe online outside of school, they are advised:
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
    - to only use moderated chat rooms that require registration and are specifically for their age group;
    - not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted as there is no control where images may end up or who can see them
    - how to set up security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.
    - not to give out personal details to anyone on-line that may help to identify or locate them or anyone else
    - not to arrange to meet anyone whom they have only met on-line or go "off-line" with anyone they meet in a chat room
    - to behave responsibly whilst on-line and keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken.

Robson House School website

- All content uploaded onto the Robson House website has been authorised by the online safety co-ordinator and the heads of school, who are responsible for ensuring that content is accurate, suitable for the purpose and audience, and does not breach copyright or intellectual property law.

- At Robson House, Darryl Jones, Head of School is the designated person who has responsibility for uploading materials onto the website.

- To ensure the privacy and security of staff and children, the contact details on the website are the school address, email and telephone number. No direct contact details for staff or children are contained on the website.

- Children's full names or photos are never published on the website.

- Links to any external websites are regularly reviewed to ensure that their content is appropriate for the school and the intended audience.

Photographic and video images

- Where Robson House uses photographs and videos of children for publicity purposes, for example on the school website, images are carefully selected so that individual children cannot be easily identified. (e.g. no photos of a child's face).

- Where photographs or videos of children are used, written permission must be obtained first from their parents or carers, who are informed of the purpose of the image and where it will appear.

- Children's names are never published where their photograph or video is being used.

- Staff ensure that children are suitably dressed to reduce the risk of inappropriate use of images.

- Images are securely stored only on the school's computer system and all other copies deleted.

- Staff do not use personal devices to take photographs of children.

- Stored images should not be labelled with the child's name.

- Robson House inform parents that they may not take photographic images of school events that include other children.

Children's own mobile devices

The majority of children are likely to have mobile phones or other devices that allows them to access internet services, and these can pose a major problem for schools in that their use may distract children during lessons and may be used for online bullying.

However, many parents prefer their children to have mobile phones with them in order to ensure their safety and enable them to contact home if they need to. The use of personal mobile phones or other devices is forbidden in classrooms and children who bring their own devices into Robson House are required to hand these into the office for the duration of the school day. They are returned at the end of the day.

Where a pupil's device is used for bullying or sexual harassment, schools we will confiscate the device so that evidence can be gathered. We can also refer to the government guidance available at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

Staff are not allowed to use their own devices when they are with the children. Staff devices must be on silent and in a safe space so as not to disrupt the school day. There are notices around the school explaining that people are not allowed to use their phones in these areas. This applies to parents/carers as well as visitors.

4 Remote Learning

Through the use of Information and Communications Technology (ICT), Some forms of learning may occur at home. Where deemed appropriate the school may provide children with access to remote learning. Remote learning involves engaging in a wide range of learning activities, and includes the use of ICT and use a mixture of familiar learning techniques and traditional methodologies and will be delivered entirely online. The school will provide remote learning opportunities under exceptional circumstances and it's appropriateness for a child will be assessed on a case by case basis by the heads of school. The Curriculum Lead manages the schools remote learning capabilities and the Online Safety Coordinator will continue to be responsible for safe IT arrangements

Robson house uses Google Classroom and Zoom to provide remote leaning access to both staff and students. Google Classroom will be used to assign academic work, resources and provide marking and feedback. Zoom will be used to provide the staff and children the opportunity to have one to one contact during a time of remote learning and staff members may also live stream lessons and provide online mentoring for children.
Staff and children will have access to remote learning with the use of their unique Robson House logins. Staff and children and parents/carers will be trained to use the appropriate software. In accordance with the schools equalities policy remote learning where deemed appropriate will be customised to meet the individual needs of the child.

Live streaming

Livestreaming can be used by the school to broadcast an event taking place in school such as an educational lesson or an online mentoring session. It's a valuable educational medium which can connect a child with the school when providing remote learning solutions.

To create a safe environment for children and young people when watching or engaging in a livestream, it is the responsibility of the staff to teach children online safety specifically in regards to live streaming. Staff members will follow the guidance mentioned in the Responsibilities section on the Online Safety Policy. In the introductory phase of remote learning, children will be reminded:

- not to share private information
- not to respond to contact requests from people they don't know
- who they should tell if they see or hear anything upsetting or inappropriate
- Neutral space for teaching and learning

Hosting a live stream

Hosting a livestream means any situation where the school instigates, publishes and is responsible for streaming online content. This includes livestreaming lessons, assemblies, announcements, activities, and if external visitors livestream on the school site. Any form of Livestream performed by the school (including name of child and staff member) will be recorded in the whole school calendar in advance. Any changes, absences will also be recorded in the whole school calendar. Any form of live stream facilitated by the school will also be recorded in its entirety and saved in the school system.

Safe use of technology in remote learning

Robson House is committed to providing a safe and secure environment for children. Some of the measures to be followed during remote learning includes:

- During any remote learning activity staff members are instructed to follow the schools safeguarding policy and protocols. Online safety incidents involving safeguarding issues, for example contact the Designated Safeguarding Lead and report it on My Concern. More information can be found in the schools safeguarding policy.
- All sessions will be timetabled on the Whole School Calendar and any changes will be also noted.
- Parents and carers will be provided with information on any web sites the children might be asked access to research and complete any remote learning task.

Further guidance on Remote learning can be found in our remote learning policy and on the London Grid for Learning website: https://www.lgfl.net/online-safety/

5 Responding to incidents

Policy statement

- All incidents and complaints relating to online safety and unacceptable internet use will be reported to the online safety co-ordinator in the first instance. All incidents, whether involving children or staff, must be recorded by the online safety co-ordinator on the online safety incident report form (appendix 3).

- A copy of the incident record will be emailed to Camden's designated online safety officer at jenni.spencer@camden.gov.uk.

- Where the incident or complaint relates to a member of staff, the matter will always be referred to the executive head teacher for action under the staff conduct policy for low level incidents or consideration given to contacting the LADO under the CSCP guidance on dealing with allegations against staff where this is appropriate. Incidents involving the executive head teacher will be reported to the chair of the management committee

- The Robson House online safety co-ordinator keeps a log of all online safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's online safety system, and use these to update the online safety policy. These are recorded on the My Concern online system.

- Online safety incidents involving safeguarding issues, for example contact with inappropriate adults, are reported to the designated people for safeguarding who will make a decision as to whether or not to refer the matter to the police and/or Children's Safeguarding and Social Work in conjunction with the executive head teacher.

Although it is intended that online safety strategies and polices should reduce the risk to children whilst on-line, this cannot completely rule out the possibility that children may access unsuitable material on the internet. Neither the school nor the London Borough of Camden can accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment.

Unintentional access of inappropriate websites

- If a child or member of staff accidently opens a website that has content which is distressing or upsetting or inappropriate to the children' age, staff will immediately (and calmly) close or minimise the screen.

- Staff should reassure children that they have done nothing wrong and discuss the incident with the class to reinforce the online safety message and to demonstrate the school's "no blame" approach.

- The incident will be reported to the online safety co-ordinator and details of the website address and URL provided.

- The online safety co-ordinator will liaise with the network manager or learning platform provider to ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.

Intentional access of inappropriate websites by a child

- If a child deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions (see section 5).
- The incident will be reported to the online safety co-ordinator and details of the website address and URL recorded.
- The online safety co-ordinator will liaise with the network manager or learning platform provider to ensure that access to the site is blocked.
- The child’s parents will be notified of the incident and what action will be taken.

Inappropriate use of IT by staff

- If a member of staff witnesses misuse of IT by a colleague, they will report this to the executive head teacher and the online safety co-ordinator immediately. If the misconduct involves the executive head teacher or a member of the management committee the matter will be reported to the chair of the management committee.
- The online safety co-ordinator will notify the network manager so that the computer, laptop or other device is taken out of use and securely stored in order to preserve any evidence. A note of any action taken will be recorded on the online safety incident report form.
- The online safety co-ordinator will arrange with the network manager or learning platform provider to carry out an audit of use to establish which user is responsible and the details of materials accessed.
- Once the facts are established the executive head teacher will take any necessary disciplinary action against the staff member and report the matter to the management committee and the police where appropriate. Where appropriate, consideration should be given to contacting the LADO for advice.
- If the materials viewed are illegal in nature the executive head teacher will report the incident to the police and follow their advice, which will also be recorded on the online safety incident report form.

Online bullying

Definition and description

Online bullying is defined as the use of technology such as email and social networking sites to deliberately hurt or upset someone or harass or threaten. Unlike physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

Online bullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous.

Bullying may take the form of:

- rude, abusive or threatening messages via email or text
- posting insulting, derogatory or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making or sharing derogatory or embarrassing images or videos of someone via mobile phone or email (for example, sexting/"happy slapping").

Online bullying can affect children and staff members. Often, the internet medium used to perpetrate the bullying allows the bully to remain anonymous. In extreme cases, online bullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.

Dealing with incidents

The following covers all incidents of bullying that involve children at Robson House whether or not they take place on school premises or outside school. All incidents are dealt with under the schools' behaviour policies and the peer on peer abuse guidance. https://cscp.org.uk/professionals/schools-and-nurseries-safeguarding-policies/

- Robson House anti-bullying and behaviour policies and acceptable use policies should cover the issue of online bullying and set out clear expectations of behaviour and sanctions for any breach.

- Any incidents of online bullying are reported to the online safety co-ordinator who will notify record the incident on the incident report form and ensure that the incident is dealt with in line with the Robson House anti-bullying policy. Incidents are monitored and the information used to inform the development of anti-bullying policies.

- Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration will be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.

- As part of online safety awareness and education, children are told of the "no tolerance" policy for online bullying and encouraged to report any incidents to school staff.

- Children are taught:
  - to only give out mobile phone numbers and email addresses to people they trust
  - to only allow close friends whom they trust to have access to their social networking page

    - not to send or post inappropriate images of themselves
    - not to respond to offensive messages
    - to report the matter to their parents/carers and school staff immediately.

Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.

Any action taken on online bullying incidents is proportional to the harm caused e.g. for some cases, it may be more appropriate to help the children involved to resolve the issues themselves rather than impose sanctions.

Action by service providers

All website providers and mobile phone companies are aware of the issue of online bullying and have their own systems in place to deal with problems, such as tracing communications. School staff or parents/carers can contact providers at any time for advice on what action can be taken.

- Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls. The child should also consider changing their phone number.

- Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced. The child should also consider changing email address.

- Where bullying takes place in chat rooms or gaming sites, the child should leave the chat room or gaming site immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.

- Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully’s access to the site can be blocked.

- Parents/carers are always notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.

Online bullying of staff

- The executive head teacher at Robson House is aware that school staff may become victims of online bullying by children and/or their parents. Because of the duty of care owed to staff, the executive head teacher ensures that staff are able to report incidents in confidence and receive adequate support, including taking any appropriate action against children and parents.

- The issue of online bullying of staff is incorporated into any anti-bullying policies, education programme or discussion with children so that they aware of their own responsibilities.

- Incidents of online bullying involving staff is recorded and monitored by the online safety co-ordinator in the same manner as incidents involving children.

- School staff will follow the guidance on safe IT use in section 3 of this policy and avoid using their own mobile phones or email addresses to contact parents or children so that no record of these details becomes available.

- Personal contact details for school staff are not posted on the school website or in any other school publication.

- Staff will follow the advice above on online bullying of children and not reply to messages but report the incident to the executive head teacher immediately.

- Where bullying is being carried out by parents the executive head teacher will contact the parent(s) to discuss the issue. A home/school agreement with the parent(s) will be used to ensure responsible use.

Harmful sexual behaviour online

The internet contains a high level of sexually explicit content and internet-based communications systems and social networking sites can be used to send sexually explicit messages and images. In some cases these actions may be harmful or abusive or may constitute harassment or online bullying.

Schools should be aware of online behaviours of a sexual nature that could constitute harmful behaviour:

- sharing explicit and unwanted content and images
- upskirting
- sexualised online bullying
- unwanted sexualised comments and messages
- sexual exploitation, coercion or threats.

“Sexting” or the sending of sexual images between young people via the internet or mobile devices is a particular issue young people need to know that producing and sharing these images is illegal. Children need to understand that once the image is sent, they have lost control of who it is distributed to and how it is used, and that there is a good chance that the image will be widely seen, possibly including parents.

Staff need to be able to react to incidents in a proportional manner so that the welfare of young people is safeguarded and no young person is unnecessarily criminalised. Guidance for responding to incidents is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

Staff are aware of the use of IT by older children for the purpose of distributing unsuitable materials and sexually harassing other children and be able to safeguard children from this.

Staff are aware of the duty under statutory guidance *Keeping children safe in education* and *Sexual violence and sexual harassment between children in schools and colleges* which requires schools to have policies in place to deal with incidents of on-line sexual harassment. Schools should refer to the CSCB *Sexually harmful behaviour protocol* for further details. https://cscb-new.co.uk/?page_id=8266

Staff are also be aware that any of these behaviours may be
linked to the sexual exploitation of a child or is being carried out as a gang-related activity. Staff should refer to the CSCB child sexual exploitation
guidance for further details.
https://cscp.org.uk/wp-content/uploads/2020/11/CSCP-multi-agencyguidanceon-child-sexual-exploitation-2020.pdf

Risk from inappropriate contacts with adults

Teachers may be concerned about a child being at risk as a consequence of their contact with an adult they have met over the internet. The child may report inappropriate contacts or teachers may suspect that the child is being groomed or has arranged to meet with someone they have met on-line.

School staff should also be aware of children being sexually abused on-line through video messaging such as Skype. In these cases, perpetrators persuade the young person concerned to carry out sexual acts while the perpetrator watches/records.

- All concerns around inappropriate contacts should be reported to the online safety co-ordinator and the designated safeguarding leads.

- The designated safeguarding lead should discuss the matter with the referring teacher and where appropriate, speak to the child involved, before deciding whether or not to make a referral to Children's Safeguarding and Social Work and/or the police.

- The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.

- The designated safeguarding lead can seek advice on possible courses of action from Camden's online safety officer in Children's Safeguarding and Social Work.

- Teachers will advise the child how to terminate the contact and change contact details where necessary to ensure no further contact.

- The designated safeguarding lead and the online safety co-ordinator should always notify the child's parents of any concerns or incidents and where appropriate, arrange to meet with them discuss what action they can take to ensure their child's safety.

- Where inappropriate contacts have taken place using school IT equipment or networks, the online safety co-ordinator should make a note of all actions taken and contact the network manager or learning platform provider to ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other children is minimised.

Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences and maybe radicalised as a result of direct contact with online extremists or because they self-radicalise having viewed extremist materials online.

All schools have a duty under the Government's Prevent programme to prevent vulnerable young people from being radicalised and drawn into terrorism. The main mechanism for this is Camden's Channel Panel, a multi-agency forum that identifies young people who are at risk and develops a support plan to stop the radicalisation process and divert them from extremism.

- Staff are aware of the school's duty under the Prevent programme and are able to recognise any child who is being targeted by violent extremists via the internet for the purposes of radicalisation. Children and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- Robson House will ensure that adequate filtering is in place and review filtering in response to any incident where a child or staff member accesses websites advocating violent extremism.

- All incidents will be dealt with as a breach of the acceptable use policies and the Robson House's behaviour and staff disciplinary procedures should be used as appropriate.

- The online safety co-ordinator and the designated leads for safeguarding will record and review all incidents in order to establish whether there are any patterns of extremist groups targeting Robson House and whether current school procedures are robust enough to deal with the issue.

- Where there are concerns that a young person is being radicalised or is in contact with violent extremists, or that their parents are and this is placing the child or young person at risk, schools should refer the young person to the Channel Co-ordinator for support.

Further information is available in the CSCB guidance “Safeguarding children and young people from radicalisation and extremism” available at: https://cscp.org.uk/resources/radicalisation-and-extremism-resources/

Risk from sites advocating suicide, self-harm and anorexia

Some internet sites advocate dangerous activities such as self-harming, suicide or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

- Robson House will ensure that young people have an opportunity to openly discuss issues such as self-harming, suicide, substance misuse and anorexia as part of the PHSE curriculum.

- Pastoral support will be made available to all young people to discuss issues affecting them and to establish whether their online activities are an added risk factor

- Staff receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

5 Sanctions for misuse of school IT

Category A infringements

These are low-level breaches of acceptable use agreements such as:

- use of non-educational sites during lessons
- unauthorised use of email or mobile phones
- unauthorised use of prohibited sites for instant messaging or social networking.

Sanctions include referral to the online safety co-ordinator and contacting parents/carers

Category B infringements

These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of online safety policy that are non-deliberate, such as:

- continued use of non-educational or prohibited sites during lessons
- continued unauthorised use of email, mobile phones or social networking sites during lessons
- use of file sharing software
- accidentally corrupting or destroying other people's data without notifying staff
- accidentally accessing offensive material without notifying staff.

Sanctions include:

- referral to online safety co-ordinator
- loss of internet access for a period of time
- banning of bringing mobile phone into school
- contacting parents.

Category C infringements

These are deliberate actions that either negatively affect Robson House's ICT systems or are serious breaches of acceptable use agreements or anti-bullying policies, such as:

- deliberately bypassing security or access
- deliberately corrupting or destroying other people's data or violating other's privacy
- online bullying
- deliberately accessing, sending or distributing offensive or pornographic material
- purchasing or ordering items over the internet
- transmission of commercial or advertising material.

Sanctions include:

- referral to online safety co-ordinator
- referral to executive head teacher
- loss of access to the internet for a period of time
- contact with parents
- any sanctions agreed under other school policies. e.g. the schools anti bullying policy

Category D infringements

These are continued serious breaches of acceptable use agreements following warnings or deliberately accessing and distributing banned or illegal materials which may result in a criminal offence, such as:

- persistent and/or extreme online bullying
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- bringing the school name into disrepute.

Sanctions include:

- referral to executive head teacher
- contact with parents
- possible fixed term exclusion
- removal of equipment
- referral to community police officer
- referral to Camden's online safety officer.
- Referral to Children's and Safeguarding Social work services
- Loss of internet access for a period of time

Sanctions for staff

Sanctions reflect the seriousness with which any breach of acceptable use policies by staff members will be viewed given their position of trust and the need to ensure acceptable standards of behaviour by adults who work with children. Sanctions will be linked to the staff code of conduct and The safer recruitment and staff conduct policy.

Category A infringements

These are minor breaches of Robson House's acceptable use policy which amount to misconduct and will be dealt with internally by the executive head teacher as a low level incident in line with the school's staff conduct policy.

- excessive use of internet for personal activities not connected to professional development
- use of personal data storage media (e.g.: removable memory sticks) without carrying out virus checks
- any behaviour on the world wide web and social media sites such as Twitter that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or children or inappropriate material published on social networking sites
- sharing or disclosing passwords to others or using other user's passwords
- Breaching copyright or licence by installing unlicensed software.

Sanctions include referral to the executive head teacher who will issue a verbal or written warning.

Category B infringements

These infringements involve deliberate actions that undermine safety on the internet and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies such as the police or Camden's LADO under the CSCP guidance on dealing with allegations against staff and volunteers. https://cscp.org.uk/professionals/managing-allegations-against-staff-and-volunteers-lado/

- serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
- any deliberate attempt to breach data protection or computer security rules, for example hacking
- deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- receipt or transmission of material that infringes the copyright of other people or is in breach of the Data Protection Act
- Bringing the school name into disrepute.

Sanctions include:

- referral to the executive head teacher
- removal of equipment
- referral to Camden's online safety officer
- referral to Camden's LADO or the police
- suspension pending investigation
- disciplinary action in line with school policies.

Appendix 1:

Acceptable use policy for children

Name:
School:
Class:

I want to stay safe while I am using a computer and I know that anything I do on the computer may be seen by someone else.

I will:

- keep my password a secret
- only open pages which my teacher has said are okay
- tell my teacher if anything makes me feel scared or uncomfortable
- make sure all the messages I send are polite
- tell my teacher if I get a nasty message
- not reply to any nasty message which makes me feel upset or uncomfortable
- not give my mobile number, home number or address to anyone who is not a real friend
- only email people I know or if my teacher agrees
- only use my school email address
- talk to my teacher before using anything on the internet
- not tell people about myself on-line (I will not tell them my name, anything about where I live or where I go to school)
- not load photographs of myself onto the computer
- never agree to meet a stranger.

Parents

- I have read the above school rules for responsible internet use and agree that my child may have access to the internet at school. I understand that the school will take all reasonable precautions to ensure children do not have access to inappropriate websites, and that the school cannot be held responsible if children do access inappropriate websites.

- I agree that my child's work can be published on the school website.

- I agree that photographs that include my child may be published but that any photography will not clearly identify my child and that their name will not be published.

Signed:

Date:

Appendix 2:

Acceptable use policy for staff and members of management committee

Access and professional use

- All computer networks and systems belong to the school and are made available to staff and members of management committee for educational, professional, administrative and governance purposes only.

- Staff and members of management committee are expected to abide by all school online safety rules and the terms of this acceptable use policy. Failure to do so may result in disciplinary action being taken against staff or members of management committee being removed.

- The school reserves the right to monitor internet activity and examine and delete files from the school's system.

- Staff and members of management committee have a responsibility to safeguard children in their use of the internet and reporting all online safety concerns to the online safety co-ordinator.

- Copyright and intellectual property rights in relation to materials used from the internet must be respected.

- E-mails and other written communications must be carefully written and polite in tone and nature.

- Anonymous messages and the forwarding of chain letters are not permitted.

- Staff and members of management committee will have access to the internet as agreed by the school but will take care not to allow children to use their logon to search the internet.

Data protection and system security

- Staff and members of management committee should ensure that any personal data sent over the internet will be encrypted or sent via secure systems. Where personal data is taken off the school premises via laptops and other mobile systems, the information must be encrypted beforehand.

- Use of any portable media such as USB sticks or CD-ROMS is permitted where virus checks can be implemented on the school ICT system using SOPHOS software.

- Downloading executable files or unapproved system utilities will not be allowed and all files held on the school ICT system will be regularly checked.

- Sharing and use of other people's log-ins and passwords is forbidden. Users should ensure that they log-out when they have finished using a computer terminal.

- Files should be saved, stored and deleted in line with the school policy.

Personal use

- Staff and members of management committee should not browse, download or send material that could be considered offensive to colleagues and children or is illegal.

- Staff and members of management committee should not allow school equipment or systems to be used or accessed by unauthorised persons and keep any computers or hardware used at home safe.

- Staff and members of management committee should ensure that personal websites or blogs do not contain material that compromises their professional standing or brings the school's name into disrepute.

- School ICT systems may not be used for private purposes without permission from the executive head teacher.

- Use of school ICT systems for financial gain, gambling, political purposes or advertising is not permitted.

I have read the above policy and agree to abide by its terms.

Name:

School:

Signed:

Date:

Appendix 3:

Online safety incident report form

This form should be kept on file and a copy emailed to Camden’s online safety officer at jenni.spencer@camden.gov.uk

School/organisation’s details:

Name of school/organisation:

Address:

Name of online safety co-ordinator:

Contact details:

Details of incident

Date happened:

Time:

Name of person reporting incident:

If not reported, how was the incident identified?

Where did the incident occur?
□ In school/service setting □ Outside school/service setting

Who was involved in the incident?
□ child/young person □ staff member □ other (please specify

Type of incident:
□ bullying or harassment (online bullying)
□ deliberately bypassing security or access
□ hacking or virus propagation
□ racist, sexist, homophobic religious hate material
□ terrorist material
□ drug/bomb making material
□ child abuse images
□ on-line gambling
□ soft core pornographic material
□ illegal hard core pornographic material
□ other (please specify)

Nature of incident

□ **Deliberate access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Could the incident be considered as;
□ harassment □ grooming □ online bullying □ breach of AUP

□ **Accidental access**

Did the incident involve material being;
□ created □ viewed □ printed □ shown to others
□ transmitted to others □ distributed

Action taken

□ **Staff**

□ incident reported to executive head teacher/senior manager
□ advice sought from Family Services and Social Work
□ referral made to Family Services and Social Work
□ incident reported to police
□ incident reported to Internet Watch Foundation
□ incident reported to IT
□ disciplinary action to be taken
□ online safety policy to be reviewed/amended

Please detail any specific action taken (ie: removal of equipment)

□ **Child/young person**

□ incident reported to executive head teacher/senior manager
□ advice sought from Family Services and Social Work
□ referral made to Family Services and Social Work
□ incident reported to police
□ incident reported to social networking site
□ incident reported to IT
□ child's parents informed
□ disciplinary action to be taken
□ child/young person debriefed
□ online safety policy to be reviewed/amended

Outcome of incident/investigation